METHOD AND SYSTEM FOR AUTHENTICATION WHEN CERTIFICATION AUTHORITY PUBLIC AND PRIVATE KEYS EXPIRE

Field of the invention:

This invention relates to a method and system for a solution to the problems arising from the expiry of digital certificates of the certifying authority used in a secure communication environment over a public network such as the internet.

Background of the invention:

Digital Certificates are used all over the Secure Internet world for Authentication and Data Integrity. To set up a secure Web Server, the servers request a certificate from Certification Authorities (CA). CAs are trusted third parties that are recognized and trusted by all Internet population including all Web Servers and Web Browsers. The Server Certificate is a signature by the CA that the Server has been validated by it and can be trusted. It is a signature by the CAs private key on the server's public key, its Domain Name and other information like Address etc. The self-signed Certificates of the CAs are provided in all the Servers and Browsers. So in a normal SSL Handshake between a web server and a client i.e. a Browser, when the server presents its certificate to the browser the Browser software validates the Certificate by checking the signature of the CA on the certificate with the help of the CA certificate it has.

The Problem in the above digital certificates is that the strength of the security lies in the strength of the keys used in the system. There are one pair of keys for each entity including the CA and the Web Server - the Private Key and the Public Key. Now as the CA certificates are available publicly and trusted by everyone, these keys need to be very strong and no one should be able to break them. However, this is not possible forever. Knowing the Public Key (available

in the CA Certificate), with some time and money, the keys can be broken. Each key has its own lifetime after which it is assumed that it is no longer safe to use them as in that time period the keys can be broken. So the CAs expire their certificates after some amount of time. This poses some problems as the servers using the Certificates from CAs whose certificates expire become no longer valid (even though the servers certificates are valid i.e. not expired). Although the communication might still be secure, the client throws up a message box to the user warning him that the CA has expired and it might not be a safe to transact with the server. This creates a lot of confusion for the user.

The first solution to the above problem currently is to get a new certificate for the Web server from the CA with the new CA keys generated.

The second solution to the above problem is to modify the browser software to automatically accept this connection even though the certificate has expired.

This problem was seen on 1st January 2000 very much as one of the most used Verisign Certificate expired on the day and Sites using the certificates issued by the CA has to face problems as their users got an undesired pop up window from Browsers warning them of the expiration. The solution was either get the new Server Certificate from Verisign or use New versions of the Browsers. The new versions probably accepted the certificate irrespective of the date expiration. As there are a lot of CAs, each will have the same problem when their certificates expire. The users will have problems with the old versions of the Browsers, which might amount to a sizable amount of a Web Site's users. Verisign had advised users to get the newer versions of the browser.

The third solution would be to have a requirement for all CAs not to issue Certificates for period spanning more than their expiry date.

The problem with the first Solution is that it requires generating of a new Server Certificate Request, Sending it to the CA, the CA validating and signing it, sending the Certificate to the server, and finally the server importing it and making it the default Certificate. This amounts to a lot of rework, in fact requires the entire process of Certificate generation to be done again.

The problem with the second solution is that it will work only with the newer versions of the Browser software thereby cutting a sizable amount of the Internet Population. Generally while dealing with Internet applications, users would not like to spend much time in downloading new software or might not like being advised of getting a new Browser. So sites might lose on some of their customers and hence some of their Business. Secondly, by accepting the expired CA, the newer versions defeat the purpose of having expired the Certificate at the first place and do pose a security threat.

The problem with the third solution is that it is practically not feasible and is not used currently. There are a lot of situations where CAs have to issue certificates for longer times. For e.g., the CA might generate keys for 2 years, after 1 year and 1 month, when an entity requests for a certificate for 1 year, the CA has to issue it for 1 year and cannot do that for 11 months and expect the user to get it reissued after that. The user will go to some other CA and the CA will lose its business.

Objects and Summary of the invention:

The object of this invention is to obviate the above drawbacks by providing a server certifying authority chain certificate (SCAC certificate), which is issued by the certifying authority using its new keys, to validate the previously issued server certificate.

To achieve the said objective, this invention provides a method for enabling the use of valid authentication certificates when the private key and public key of any of the certifying authorities have expired comprising:

- obtaining a server certifying authority chain (SCAC) certificate by the server from the said certifying authority,
- presenting the original valid authentication certificate along with the said server certifying authority chain certificate, by the server to the browser during the SSL handshake,
- accepting the transaction by the browser after verification of the original authentication certificate using the expired public key of the certifying authority, and verifying the said SCAC certificate using the new public key of the said certifying authority.

The said server certifying authority chain (SCAC) certificate is obtained by each server whenever the certifying authority invalidates its public key, by:

- contacting the certifying authority using the server's private key for authentication,
- verifying the request by the certifying authority using the server's public key,
- generating the SCAC certificate by the certifying authority using its new private key and forwarding to the said server.

The generating of the said SCAC certificate includes the authentication of the server name and the server public key, old certifying authority public key and certifying authority name.

The certifying authority in case of client will also issue client certificates known as (CCAC) certificates, which will work the same way as (SCAC) certificates.

During SSL handshake when the client presents its certificate, it will also present the CCAC certificate to the server.

In an arrangement of networked server and browser systems conducting secure transactions and including a certifying authority for authenticating such transactions, characterized in that it includes a means for authenticating transactions when the public and private key of the said certifying authority have expired but the authentication certificates of any of server or browser systems is still valid, comprising:

- a means for the server to obtain a certifying authority chain certificate using the new private key of the certifying authority,
- a means for presenting the said certifying authority chain certificate together with the original authentication certificate, to the browser,,
- a means for verifying the original authentication certificate using the expired public key of the certifying authority, and verifying the certifying authority chain certificate using the new certifying authority public key by the browser.

The said means for the server to obtain a SCAC certificate from the said certifying authority whenever the said certifying authority withdraws its public key comprising:

- a means for contacting the said certifying authority and requesting certifying authority chain certificate using the server's private key for authentication,
- a means for verification of the request by the certifying authority,
- a means for generating and forwarding the certifying authority chain certificate to the server by the said certifying authority.

The said certifying authority have means to generate the said SCAC certificate containing authentication of the server name and the server public key, old certifying authority public key and certifying authority name.

The said certifying authority have also means to issue client certificate known as (CCAC) certificates, which will work the same way as the (SCAC) certificate.

The system includes means to present CCAC certificates to the server during SSL handshake when the client presents its certificate.

Brief Description of the Drawings:

The invention will no be described with reference to the accompanying drawings:

Fig. 1 shows the flow diagram of the method for authenticating the server using the SCAC certificate.

Fig. 2 shows a flow diagram of a method for obtaining SCAC certificate from the certifying authority.

Detailed Description of the Drawings:

Referring to the drawings, fig. 1 shows the server presenting the valid server certificate (1.1) encrypted with the old CA public key along with the SCAC certificate (1.2) signed with a new private key, to the browser. The browser verifies the server certificate using the old CA certificate.

If the validation is unsuccessful, the transaction is rejected (3). If the verification is successful, then the browser verifies that SCAC certificate (4)

using the new CA public key. If this verification is unsuccessful, the transaction is rejected (3) but if it is successful, the transaction is accepted (5).

In fig. 2 the server periodically checks (6 & 7) for the expiry of the certifying authority Public key. If the public key has not expired, no further action is required. If however, the certifying authority public key has expired. The server sends a request (9) to the certifying authority for issuance of an SCAC certificate. This request is encrypted using the server's private key. The certifying authority verifies the authenticity of the request by checking the request using the server's public key and issues the SCAC certificate (10), if the verification is successful. This SCAC certificate is signed using the certifying authority's new private key.

The above solution can be expanded to have chains of certificates.

The above solution will also work for Client Certificates issued by the CAs and will be known as **Client CA Chain Certificates** (CCAC) and will work exactly the same way as SCAC Certificates. The Clients can keep track of the expiry of CAs who signed their Certificates, and request for a CCAC Certificate from the CA. The CA will give / generate CCAC certificates for the clients. During SSL Handshake, when the client presents its certificate, it will also present the CCAC Certificate to the Server.

Advantages:

1. By using the above method a new certificate is not required.
2. The security is not compromised. If a hacker is able to break the old CA key, he / she will not be able to break the web site certificate as he will not be able to duplicate the New Certificate issued by the new CA Keys.